GEOFFREY S. BERMAN
United States Attorney for the
Southern District of New York
By: CHRISTOPHER B. HARWOOD
CALEB HAYES-DEATS
Assistant United States Attorneys
86 Chambers Street, Third Floor
New York, New York 10007
Telephone: (212) 637-2728/2699
Fax: (212) 637-2686
christopher.harwood@usdoj.gov
caleb.hayes-deats@usdoj.gov

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

THE UNITED STATES DEPARTMENT OF THE TREASURY, Plaintiff, vs. U.S. BANK NATIONAL ASSOCIATION, Defendant.	No. 18 Civ. 1358 COMPLAINT Jury Trial Demanded

1. Plaintiff the United States Department of the Treasury (the "Government"), by its attorney, Geoffrey S. Berman, United States Attorney for the Southern District of New York, brings this action against U.S. Bank National Association ("US Bank" or the "Bank") under the Currency and Foreign Transactions Reporting Act of 1970, as amended, 31 U.S.C. § 5311 *et seq.*, which is commonly referred to as the Bank Secrecy Act (the "BSA"), and its implementing regulations.

2. On February 15, 2018, the Financial Crimes Enforcement Network ("FinCEN"), a component of the United States Department of the Treasury, assessed a civil money penalty of $185 million (the "assessment") against US Bank. The assessment charges US Bank with

willfully violating the BSA and its implementing regulations. Through this action, the Government seeks an order: (1) reducing the assessment to judgment; and (2) requiring US Bank to meet with FinCEN annually for a period of two years to: (a) identify all remedial actions the Bank has taken during the preceding calendar year to address prior deficiencies related to its allocation of resources (including sufficient staff) to its anti-money laundering ("AML") program, and explain why existing resource levels are sufficient to maintain compliance with the BSA; and (b) identify the independent testing that has been conducted (either internally or externally) during the preceding calendar year on the BSA functions at the Bank, including model validation of its transaction monitoring software and reviews of its processes and procedures regarding alert generation, investigation of alerts, and disposition of alerts. In support, the Government alleges as follows:

INTRODUCTION

3. Starting in at least 2011 and continuing until 2014, US Bank failed to establish and implement an adequate AML program and file timely suspicious activity reports ("SARs"). Starting in 2014 and continuing until 2015, US Bank failed to file complete and accurate currency transaction reports ("CTRs").

4. First, in violation of 31 U.S.C. § 5318(h), the Bank failed to implement and maintain an adequate AML program. Specifically, in violation of the BSA requirement to implement adequate internal policies, procedures and controls, the Bank adopted AML policies, procedures, and controls that were deficient and caused it to fail to investigate and report suspicious activity. Such policies, procedures, and controls included (1) caps on the number of transactions that US Bank's automated transaction monitoring system would identify for review as potentially related to suspicious activity, (2) failing to include Western Union money transfers

processed at the Bank in the automated transaction monitoring system, and (3) having a customer risk-rating program that failed to include important information about its clients in its risk-rating analysis, such as a customer's country of citizenship and occupation. In addition, US Bank employed an insufficient number of AML investigators, thus violating the BSA's requirement that it not only designate a compliance officer, but also ensure that its compliance function had the resources necessary to fulfill its responsibilities. As described below, even when the Bank had more than $340 billion in assets, it employed only 32 AML investigators. Finally, US Bank did not independently validate its automated transaction monitoring system.

5. Second, in violation of 31 U.S.C. § 5318(g), US Bank failed to timely file thousands of SARs with FinCEN. Certain Bank employees understood through internal testing that the inadequate AML policies described above caused the Bank to fail to identify and report large numbers of suspicious transactions. Subsequent analysis of the Bank's transactions has revealed that it failed to timely file thousands of SARs, including in connection with structuring and other types of potential financial crime and underlying criminal activity.

6. Third, in violation of 31 U.S.C. § 5313(a), the Bank filed more than 5,000 materially inaccurate CTRs with FinCEN. The CTR form prescribed by FinCEN during the relevant period required the Bank to identify not only the party conducting the transaction, but also the person or entity on whose behalf the transaction was conducted. In more than 5,000 cases, US Bank knew that the entity on whose behalf a transaction was conducted was a money services business ("MSB")—a high-risk customer type—but nonetheless misidentified that entity on the CTR it filed. Such misidentification frustrated law enforcement's ability to identify and track potentially unlawful behavior.

7. Under the BSA and its implementing regulations, a financial institution is liable for a civil money penalty of $25,000 for each day that it fails to implement and maintain an effective AML program. Similarly, each failure to file a timely and accurate SAR or CTR renders a financial institution liable for a civil money penalty of $25,000 or the amount of the transactions at issue (up to $100,000). Finally, FinCEN may seek injunctive relief against financial institutions to, among other things, ensure future compliance with the BSA and its implementing regulations.

JURISDICTION & VENUE

8. This Court has jurisdiction over this action under 31 U.S.C. §§ 5320 & 5321(b)(2), as well as 28 U.S.C. §§ 1331, 1345, & 1355.

9. Venue is appropriate in this district under 31 U.S.C. §§ 5320 & 5321(b)(2), and 28 U.S.C. §§ 1391(b) & 1395(a).

PARTIES

10. Plaintiff is the United States Department of the Treasury.

11. Defendant U.S. Bank National Association is the fifth largest bank in the United States, with over 3,100 branches. At all times relevant to the complaint, US Bank was a "financial institution" under 31 U.S.C. § 5312(a)(2) and a "Bank" under 31 C.F.R. § 1010.100(d).

FACTS

I. BACKGROUND

A. The Relevant Statutory and Regulatory Provisions of the Bank Secrecy Act

12. As set forth below, the BSA and its implementing regulations require, among other things, that financial institutions: (1) implement an effective AML program to prevent themselves from being used to facilitate money laundering or the financing of terrorist activities;

(2) report suspicious transactions involving potentially unlawful activity; and (3) file reports on currency transactions that aggregate more than $10,000 per day. *See* 31 U.S.C. §§ 5313(a), 5318(g) & (h); 31 C.F.R. §§ 1010.310–.314, 1020.200–.210, .310, & .320(a).

13. FinCEN is a component the Department of the Treasury. The Secretary of the Department of the Treasury has delegated to the Director of FinCEN the authority to implement and enforce compliance with the BSA, including through the promulgation of regulations. *See* 31 U.S.C. § 310(b)(2)(I); Treasury Order 180-01.

1. The Requirement to Implement an Effective AML Program

14. The BSA requires that all financial institutions establish an AML program that "includ[es], at a minimum": (1) "the development of internal policies, procedures, and controls"; (2) "the designation of a compliance officer"; (3) "an ongoing employee training program"; and (4) "an independent audit function to test [the] program[]." 31 U.S.C. § 5318(h)(1).

15. FinCEN regulations in effect at all times relevant to this case further required each financial institution to maintain an AML program that complied with "the regulation of its Federal functional regulator." 31 C.F.R. § 1020.210 (2011).

16. According to the *Bank Secrecy Act / Anti-Money Laundering Examination Manual* (the "BSA/AML Manual") published by the Federal Financial Institutions Examination Council in 2006, a bank "must have a BSA/AML compliance program commensurate with its respective BSA/AML risk profile." Accordingly, "[t]he level of sophistication of the internal controls should be commensurate with the size, structure, risks, and complexity of the bank."

17. The BSA/AML Manual provides numerous examples of risks that banks should identify and monitor. For example, the manual lists "[e]lectronic funds payment services" as among the "products and services offered by banks [that] may pose a higher risk of money

laundering." The manual further identifies different types of customers that "may pose specific risks," including "[n]on-bank financial institutions" such as "money services businesses," "[n]onresident alien[s]," and "[n]on-governmental organizations and charities."

18. Under the BSA/AML Manual, a bank's risk profile informs the steps it must take to comply with each of the BSA's requirements. To develop appropriate policies and controls, banks must identify "banking operations . . . more vulnerable to abuse by money launderers and criminals . . . and provide for a BSA/AML compliance program tailored to manage risks." Similarly, while banks must designate an individual officer responsible for ensuring compliance with the BSA, such designation is not alone sufficient. Instead, the BSA/AML Manual notes that banks are responsible for ensuring that their compliance functions have "resources (monetary, physical, and personnel) [necessary] to administer an effective BSA/AML compliance program based on the bank's risk profile." Finally, a bank's independent audit program "should be risk based and evaluate the quality of risk management for all banking operations, departments, and subsidiaries."

2. The Requirement to Report Suspicious Activity

19. The BSA authorizes FinCEN to "require any financial institution, and any director, officer, employee, or agent of any financial institution, to report any suspicious transaction relevant to a possible violation of law or regulation." 31 U.S.C. § 5318(g)(1).

20. At all times relevant to this case, by regulation, FinCEN required banks to file a SAR on any transaction involving or aggregating at least $5,000 where "the bank knows, suspects, or has reason to suspect" that:

a. The transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to

violate or evade any Federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation;

b. The transaction is designed to evade any requirements of the Bank Secrecy Act or of any other regulations promulgated under the Bank Secrecy Act; or

c. The transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

31 C.F.R. § 1020.320(a).

21. Banks had an obligation to file a SAR "no later than 30 calendar days after the date of initial detection of the incident requiring the filing." *Id.* § 1020.320(b)(3). While banks could temporarily delay filing in certain circumstances, "[i]n no case shall reporting be delayed more than 60 calendar days after the date of initial detection." *Id.*

22. As set forth in the BSA/AML Manual, SARs "form[] the cornerstone of the BSA reporting system" and are "critical to the United States' ability to utilize financial information to combat terrorist financing, money laundering, and other financial crimes." Through FinCEN, law enforcement agencies may access SARs and use them to: (1) initiate investigations; (2) expand existing investigations and uncover previously unidentified co-conspirators and undetected money trails; (3) facilitate information exchange with law enforcement counterparts worldwide; and (4) identify relationships between illicit actors and their financing networks, thereby allowing the disruption of such networks and the prosecution of their participants. A bank's failure to file timely SARs deprives law enforcement of critical information it could have used for these purposes.

3. The Requirement to Report Currency Transfers

23. The BSA also authorizes FinCEN to require domestic financial institutions to file reports on transactions in currency. 31 U.S.C. § 5313(a).

24. FinCEN's regulations in effect during the period relevant to this case required "[e]ach financial institution" to "file a report of each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to such financial institution which involves a transaction in currency of more than $10,000." 31 C.F.R. §§ 1010.311, 1020.310. Financial institutions were to file such CTRs with FinCEN "within 15 days following the day on which the reportable transaction occurred," *id.* § 1010.306(a)(1) & (3), providing "[a]ll information called for" by the "forms prescribed," *id.* § 1010.306(d).

25. At all relevant times, the form FinCEN prescribed for CTRs required financial institutions to identify the "person(s) on whose behalf [the] transaction(s) is[/are] conducted." *See* FinCEN Form 104 (March 2011); *see also* 31 U.S.C. § 5313(a) ("A participant acting for another person shall make the report as the agent or bailee of the person and identify the person for whom the transaction is being made."); 31 C.F.R. § 1010.312 (requiring financial institutions to "record the identity, account number, and the social security number or taxpayer identification number, if any, of any person or entity on whose behalf [the] transaction is to be effected").

26. CTR reporting requirements play a major role in FinCEN's core mission of safeguarding the financial system from illicit use through the collection, analysis, and dissemination of financial intelligence. Because cash-intensive businesses are criminal organizations' method of choice for laundering the proceeds of illegal cash transactions, FinCEN and law enforcement rely on the accurate and timely filing of CTRs by financial institutions to establish and follow the trail that documents the movement of potentially illicit funds.

4. Enforcement of the BSA and Its Implementing Regulations

27. Under the BSA, any domestic financial institution that "willfully" violates the BSA or its implementing regulations is liable "for a civil penalty of not more than the greater of the amount (not to exceed $100,000) involved in the transaction (if any) or $25,000." 31 U.S.C. § 5321(a)(1). For violations of a financial institution's duty to implement an effective AML program, "a separate violation occurs for each day the violation continues and at each office, branch, or place of business at which a violation occurs or continues." *See id.*

28. The willfulness requirement of 31 U.S.C. § 5321(a)(1) may be satisfied by showing that the defendant acted recklessly or with willful blindness. *See United States v. Williams*, 489 Fed. Appx. 655, 658, 660 (4th Cir. 2012); *United States v. McBride*, 908 F. Supp. 2d 1186, 1204–05 (D. Utah 2012); *see generally Safeco Ins. Co. of Am. v. Burr*, 551 U.S. 47, 57–58 (2007) ("[W]here willfulness is a statutory condition of civil liability, we have generally taken it to cover not only knowing violations of a standard, but reckless ones as well . . . .").

29. FinCEN has six years from the date of the relevant underlying conduct to assess a civil money penalty under 31 U.S.C. § 5321(a)(1). *See* 31 U.S.C. § 5321(b)(1). FinCEN may commence a civil action to recover an assessed penalty "at any time before the end of the 2-year period beginning on . . . the date the penalty was assessed." *Id.* § 5321(b)(2).

30. Additionally, when FinCEN believes that a financial institution "has violated" the BSA or its implementing regulations, it may bring a "civil action in the appropriate district court of the United States . . . to enjoin the violation or to enforce compliance." *Id.* § 5320.

B. US Bank's AML Program

31. US Bank delegated the responsibility for ensuring that it met its obligations under the BSA to its AML compliance department, which it referred to internally as Corporate AML.

In 2007, the Bank named a new Chief Compliance Officer (the "CCO") and gave him responsibility for supervising Corporate AML. Shortly after that, the CCO hired a new AML Officer (the "AMLO"). In 2010, US Bank promoted the CCO to Deputy Chief Risk Officer. In his capacity as Deputy Chief Risk Officer, the CCO retained oversight over the Bank's AML program.

32. From 2004 to the end of 2014, US Bank's AML program used SearchSpace, a commercially available software system, to monitor transactions flowing through the Bank for potential money laundering and other types of illicit conduct. The automated monitoring tools that US Bank ran against the data in SearchSpace were "Security Blanket" and "Queries." Security Blanket examined transactions that fed into SearchSpace and, on a monthly basis, assigned each transaction a score to reflect the extent to which it was unusual or unexpected for the customer. The Bank began implementing Queries to complement Security Blanket in 2005. Queries were "rules" that were run against transaction data in SearchSpace to identify indicia of potentially suspicious activity.

33. Each month, Security Blanket would each generate a set of alerts. It would do so by reviewing account activity at the Bank, assigning scores to different events that reflected each event's level of potential risk, and then aggregating the event scores for individual accounts or customers. After aggregating event scores, Security Blanket would generate alerts on the accounts or customers with the highest total risk scores. Queries would also generate alerts. As described below, US Bank often imposed caps on the number of alerts Security Blanket and certain Queries would generate, which meant that certain accounts or customers with high risk scores would not generate alerts simply because the Bank had other accounts or customers with even higher risk scores. The Bank also applied a "90-day rule" that further suppressed alerts on

some accounts. Under the 90-day rule, Queries would not generate a new alert on any account that had produced an alert in the past 90 days, regardless of the score Queries attributed to the account or whether the prior alert had resulted in a SAR. After Security Blanket and Queries generated alerts, an AML investigator would review the relevant account or customer to determine, *inter alia*, whether the Bank should file a SAR.

II. US BANK WILLFULLY VIOLATED THE BSA BY FAILING TO IMPLEMENT AND MAINTAIN AN EFFECTIVE AML PROGRAM, FAILING TO FILE TIMELY SARs, AND FAILING TO FILE COMPLETE AND ACCURATE CTRs

34. As set forth below, between 2009 and May 2015, US Bank willfully violated three separate requirements imposed by the BSA. First, from 2009 until 2014, it violated the requirement that it implement and maintain an AML program capable of adequately responding to the risks associated with the Bank, given its size and the complexity of the products and services it offered. *See* 31 U.S.C. § 5318(h). Second, during the same period, the Bank failed to file SARs on thousands of transactions that a compliant, risk-based AML program would have identified and reported as suspicious. *See id.* § 5318(g). Third, between July 2014 and May 2015, US Bank filed more than 5,000 CTRs that, according to information known to the Bank, misidentified the entities on whose behalf the underlying transactions were conducted. *See id.* § 5313(a).

A. US Bank Willfully Failed to Implement a Compliant, Risk-Based AML Program

35. Between 2009 and 2014, US Bank failed to meet at least two requirements of an effective AML program. *See id.* § 5318(h)(1). As set forth in more detail below, throughout this period, the Bank had a deficient AML transaction monitoring system that, among other things, failed to conduct risk-based monitoring of its financial transactions and instead set fixed limits on the number of alerts that it would investigate for suspicious activity. The Bank also failed to

have its automated transaction monitoring system validated by a suitably independent individual (or entity). The above conduct violated the BSA requirement relating to policies, procedures, and controls. In addition, US Bank limited the number of alerts that it reviewed largely because it lacked a sufficient number of investigators in its Corporate AML department to review alerts properly, and it did not want to devote the resources necessary to hire additional staff. The Bank's failure to maintain sufficient AML staff constituted a violation of the BSA requirement relating to the designation of appropriate AML resources (including personnel).

1. US Bank Failed to Implement Appropriate AML Policies, Procedures and Controls

36. US Bank violated the BSA by failing to implement and maintain appropriate AML policies, procedures, and controls. *See* 31 U.S.C. § 5318(h)(1)(A). The Bank's AML policies, procedures, and controls failed to meet the BSA's requirements in multiple respects. As noted above, the Bank artificially limited the number of alerts that it would investigate to evaluate potentially suspicious activity and determine whether to file a SAR. Moreover, despite permitting individuals who were not US Bank customers to conduct money transfers through Western Union at the Bank's facilities, US Bank knowingly failed to incorporate such transfers into its automated system for identifying potentially suspicious transactions. Additionally, the Bank had inadequate processes and procedures for identifying and addressing high-risk customers.

a. US Bank Artificially Limited the Number of Alerts It Investigated

37. When it first began using SearchSpace, the Bank, at the recommendation of the SearchSpace vendor, configured the system so that Security Blanket would generate a fixed number of alerts per month, rather than setting a risk-based threshold that would have generated all alerts naturally occurring at or above the score corresponding to a certain level of risk. US

Bank configured Security Blanket in this manner until 2013, even after its compliance professionals were on notice through, *inter alia*, previous FinCEN guidance, that alert caps were inconsistent with industry standards.

38. Over time, even as the Bank grew in size, it reduced the number of Security Blanket alerts that it would review each month from a high of 1,500 in 2004 to 500 by 2009.

39. Similarly, although US Bank had in place only 22 different Queries, it set numerical caps on alerts arising from the six Queries that typically generated the largest volumes of alerts. The Bank continued to impose numerical caps on most of these alerts until 2014.

40. As a result of the above-referenced alert limits, US Bank's transaction monitoring system did not generate alerts for many of the transactions that a risk-based approach would have flagged as potentially suspicious. Ultimately, a significant number of alerts were not investigated, preventing suspicious activity from being reported. The OCC had repeatedly warned Bank officials that managing the Bank's monitoring programs to the size of its staff and other resources would get the Bank in trouble with the OCC. Nonetheless, the Bank failed to properly address the numerical caps because those caps, as described below, permitted the Bank to hire fewer employees and investigators in its AML department.

41. Moreover, the Bank knew that its alert limits were causing it to fail to investigate—and file SARs on—significant numbers of suspicious transactions. From 2007 through April 2012, US Bank conducted "below-threshold" testing to evaluate the extent to which the limits it placed on alerts for Queries had caused it to fail to investigate (and file SARs on) suspicious activity. The below-threshold testing involved selecting a sampling of alerts occurring immediately below the alert limits and then having investigators review them in order to determine whether the limits should be adjusted because suspicious activity was occurring

below the threshold. This below-threshold testing found a significant amount of suspicious activity occurring below the alert limits that the Bank had employed. For example, in November 2011, the Bank's AML staff concluded that, during the past year, the SAR filing rates for below-threshold testing averaged between 30% and 80%. In other words, between 30% and 80% of the transactions that were reviewed during the below-threshold testing resulted in the filing of a SAR.

42. Based on the results of the below-threshold testing, certain Bank employees wanted to lower the alert thresholds in order to increase the number of alerts reviewed and ensure that suspicious activity was properly investigated and reported. Nonetheless, the Bank failed to properly address the concerns raised by below-threshold testing. In fact, rather than reducing alert thresholds and investigating a larger number of transactions, the Bank decided stop conducting below threshold testing in April 2012. The Bank's internal explanation for that decision relied on a pretext. In reality, the Bank terminated its below-threshold testing because that testing showed that the Bank was failing to address an ongoing problem. As the AMLO wrote in a memorandum to the Bank's CCO on December 1, 2009, a "regulator could very easily argue that [below-threshold] testing should lead to an increase in the number of queries worked."

43. The CCO and AMLO recognized that the alert caps, in addition to causing the Bank to fail to investigate (and report) large amounts of potentially suspicious activity, also was at odds with the expectations of regulators. As noted above, the OCC warned US Bank on several occasions that using numerical caps to limit the Bank's monitoring programs based on the size of its staff and available resources could get the bank in trouble with the OCC.

44. To avoid regulatory problems, US Bank took steps to avoid disclosing the alert caps to the OCC. In 2012, when the Bank hired new officials to oversee its AML program, their

predecessors, including the CCO, discouraged them from removing the alert caps or disclosing them to the OCC by representing to the new officials that the OCC was fully aware of the Bank's monitoring practices and had at least tacitly approved them. More broadly, driven in large measure by instructions from the CCO, compliance employees consistently did not volunteer information to regulators, including information about deficiencies with transaction monitoring, except in response to specific requests. In 2013, the AMLO described US Bank's AML program as an effort to use smoke and mirrors to pull the wool over the eyes of the OCC.

45. Notably, in 2013, certain of the Bank's AML employees prepared a PowerPoint presentation for the Bank's CEO that identified multiple vulnerabilities in the Bank's AML program, and explained how those same problems had led the OCC to take action against other banks. The PowerPoint presentation explicitly referred to, among other things, "[m]anipulation of system output through use of alert caps on both profiling and query detection methods" that could "potentially result in missed Suspicious Activity Reports" and "[p]otential regulatory action resulting in fines, consent order, and significant historical review of transactions." However, the CCO reviewed the draft and removed references to alert caps from the presentation, added positive information about the Bank's AML program, and otherwise altered the presentation to depict a more favorable image of the Bank's AML program.

46. The Bank did not begin to address its deficient policies and procedures for monitoring transactions and generating alerts until June 2014, when, *inter alia*, questions from the OCC caused the Bank's then Chief Risk Officer to retain outside counsel to investigate the Bank's practices. At that point, the Bank had maintained inappropriate alert caps for no less than five years.

b. The Bank Knowingly Failed to Monitor Western Union Transfers

47. In addition to capping alerts, US Bank's transaction monitoring practices were also defective because the Bank failed to monitor transactions conducted at its branches through Western Union's money transfer system.

48. From May 2009 until July 2014, US Bank allowed both customers and non-customers to conduct Western Union currency transfers at US Bank branches. The Bank recognized that such currency transfers were one of the riskiest products offered by the Bank, and that, to the extent such transfers were conducted by non-customers, they would not be processed through SearchSpace (and thus would not be the subject of alerts generated by Security Blanket or Queries). The Bank nonetheless continued to process Western Union transactions for non-customers until July 2014.

49. The Western Union transactions by non-customers that US Bank failed to monitor were voluminous and posed significant risks. For example, in 2012, the Bank handled 1.1 million Western Union transactions totaling $582 million, approximately half of which were from non-customers. During 2013, a significant percentage of Western Union transactions involved countries on the Bank's Primary or Secondary High-Risk Country lists, including Nigeria, Pakistan, Colombia, Afghanistan, and Lebanon.

50. Moreover, US Bank also failed to investigate Internal Referral Forms ("IRFs") that its employees filed on potential AML issues raised by Western Union transactions. IRFs were a mechanism through which Bank employees could raise AML concerns they had identified. The IRFs were not, however, part of the automated monitoring system that served as the Bank's primary AML monitoring tool, which as noted above, did not review Western Union transactions by non-customers. Even though Bank employees had been filling out IRFs for years

in which they raised AML concerns about Western Union money transfers by non-customers, such forms were not investigated by the Bank's AML department until June 2013.

51. Bank employees understood that failing to monitor the Western Union transactions the Bank processed would violate the BSA.

52. Notably, in December 2012, the new AML Officer (who replaced the AMLO) emailed the CCO with concerns about monitoring Western Union currency transfers at the Bank. In response, the CCO dismissed the new AML Officer's concerns and chastised him for recording them in an email.

c. US Bank Had Inadequate Processes and Procedures to Identify and Address High-Risk Customers

53. US Bank also had inadequate processes and procedures to address high-risk customers. In particular, the Bank's customer risk-rating program failed to review customer relationships in their entirety — *i.e.*, across the Bank's different business lines — in order to obtain an enterprise-wide view of customer risk. In addition, the Bank failed to include important information about its clients in its risk-rating analysis, such as a customer's country of citizenship and occupation. The exclusion of this information resulted in high-risk customers being risk-rated based on incomplete information. As a result, customers whom the Bank identified or should have identified as high-risk were free to conduct transactions through the Bank with insufficient oversight.

2. US Bank Failed to Hire an Adequate Number of AML Employees

54. US Bank further violated the requirement that it implement and maintain an effective AML program by devoting an insufficient number of employees to AML compliance. *See* 31 U.S.C. § 5318(h)(1)(B). The Bank maintained its alert caps largely because the caps permitted the Bank to hire fewer AML staff, and devote fewer resources to its AML program,

than would have been necessary had the Bank implemented a risk-based approach to transaction monitoring. For example, no later than 2007, an AML employee observed: "The number of query alerts that we work are [sic] increasingly based solely on staffing levels. This is a risk item." For much of the relevant period, US Bank had only 25–30 AML investigators. During the relevant period, US Bank made no effort to meaningfully increase the size of investigative staff. Indeed, it only added AML investigators as a result of acquiring other banks. As late as 2012, when US Bank had over $340 billion in assets, the Bank had only 32 investigators.

55. US Bank also failed to pay its compliance employees the market salary. As a result, the Bank's experienced AML investigators frequently left for higher paying jobs at other institutions. US Bank failed to increase the salaries of its AML staff even after Human Resources and Compliance personnel complained to the CCO that the below-market pay enabled competitor banks to successfully poach AML investigators.

56. The CCO and AMLO understood that the Bank's failure to hire additional staff created significant AML risks. For example, the December 2009 memorandum from the AMLO to the CCO acknowledged that, even though the Bank had seen significant increases in SAR volume, law enforcement inquiries, and closure recommendations, "staffing levels have remained relatively constant." According to the AMLO, the combination of these factors resulted in an "increased workload" for "staff that already is stretched dangerously thin." The AMLO also explicitly referenced alert caps, describing the trends discussed above as "especially distressing give[n] the fact that an increase in the number of alerts worked is imminent and necessary." Nonetheless, as described above, US Bank neither removed alert caps nor hired an adequate number of AML employees for years after December 2009.

3. The Bank Failed to Independently Validate SearchSpace

57. US Bank also failed to provide for independent validation of its automated transaction monitoring system.

58. Specifically, despite recommendations and warnings from the OCC dating back to 2008, the Bank failed to have SearchSpace independently validated. For example, in connection with an OCC review of SearchSpace in 2008, the OCC found that "Management has not validated SearchSpace in accordance with OCC Bulletin 2000-16 Model Validation." The OCC discussed the results of this review with, among others, the CCO and AMLO. Thereafter, in connection with another review of SearchSpace in 2010, the OCC concluded that, although "Management [had] validated Searchspace" since the OCC's 2008 review, "the individual who completed the validation [was not] independent, given his primary responsibilities surrounding the Searchspace system." The OCC recommended that the Bank complete an independent validation of SearchSpace, and it again discussed the results of its review with, among others, the CCO and AMLO. The Bank, however, did not independently validate SearchSpace at that time.

59. Not only did the Bank fail to follow the OCC's recommendation that it conduct independent validation, but it had one of its employees conduct "validations" of SearchSpace that were plainly insufficient. After the OCC's 2010 review, and continuing into 2013, the Bank employee who was responsible for managing SearchSpace (the "SpearchSpace Manager") prepared a "biannual SearchSpace Model validation" and asked another Bank employee (the "Other Employee") to review it and acknowledge having done so, while assuring the Other Employee that he was "not making any representation that [he was] validating anything." For purposes of these biannual reviews, the Other Employee merely "read [the SearchSpace

Manager's] documentation and sign[ed] off that . . . they ma[d]e sense and that [he] believe[d] they [were] accurate."

60. While U.S. Bank was engaging in this deficient validation process, the SearchSpace Manager stated to the Other Employee that a regulator "could (and probably will at some point), force us to hire outside auditors to perform a more robust independent validation/review," but "this would cost tens of thousands . . . minimum." The SearchSpace Manager told the Other Employee that "[u]ntil we are forced to go there . . . you are sufficient."

B. US Bank Willfully Failed to File Thousands of Timely SARs

61. As described above, senior officials at US Bank understood that the deficiencies in the Bank's AML program caused the Bank to fail to identify and report suspicious transactions. Subsequent analysis has demonstrated that the Bank's defective AML practices caused it to fail to file SARs on thousands of suspicious transactions, in violation of 31 U.S.C. § 5318(g).

62. In October 2015, the Bank entered into a consent order with the OCC based on various deficiencies in its AML compliance program, including gaps in suspicious activity monitoring, insufficient staffing, and inadequate monitoring of Western Union transactions.

63. Pursuant to the consent order, the Bank performed a look-back analysis to assess the impact of the Bank's deficient monitoring practices. Specifically, the Bank reanalyzed transactions that occurred during the six months prior to taking steps to remedy these practices, including removing fixed limits on Security Blanket alerts, lifting caps on and expanding coverage of various Queries, and refusing to process Western Union transactions from non-customers.

64. As part of the look-back analysis, the Bank also reanalyzed transactions implicated by changes it had made to its processes and procedures for identifying and addressing high-risk customers. Such changes addressed, among other things, defects in the Bank's customer risk-rating program, including its above-referenced failure to review customer relationships in their entirety, as well as the Bank's failure to include important information about its clients in its risk-rating analysis.

65. The look-back analysis resulted in the generation of an additional 24,179 alerts and the filing of 2,121 SARs. The value of the transactions reported in these SARs was $719,465,772.

66. Specifically, the look-back analysis consisted of the following as it pertained to high-risk customers, Queries and Security Blanket, and Western Union transactions.

- **High-Risk Customers.** The Bank's look-back analysis concerning high-risk customers covered a six-month period between August 2014 and January 2015. As a result of this look back, the Bank late filed 136 SARs on transactions of more than $120 million.

- **Queries and Security Blanket.** The Bank's look back relating to its (1) removal of limits on Security Blanket alerts and (2) lifting of caps on and expanding coverage of various Queries covered several different six-month periods between July 2012 and June 2014. This look back resulted in the Bank late filing 987 SARs on transactions of over $220 million.

- **Western Union.** The Bank's look-back analysis concerning Western Union covered the period between January and June 2014. That analysis resulted in the Bank late filing 431 SARs on transactions involving more than $12 million.

67. As noted above, the look-back analysis covered various time periods, but did not cover the full time periods when the deficient monitoring practices were in effect. A similar analysis of the remainder of the time periods during which the Bank maintained each deficient monitoring practice would have identified additional transactions for which SARs should have been filed. Indeed, when senior management at the Bank became aware of the numerical caps on

alerts from Security Blanket and Queries in 2014, they retained a third-party consultant to analyze the impact of the caps and shared the following findings with the OCC:

- **Queries.** To test the impact of the Bank's Query thresholds, the consultant sampled 68 accounts that Queries had flagged in 2013, but that had not alerted because the accounts fell below the alert limits that were then in effect. The consultant found that 26 of the accounts (38%) were "productive or potentially productive," meaning that, for those accounts, the consultant was unable to identify a reasonable explanation for the unusual alert activity.

- **Western Union.** The consultant also tested a sample of IRFs that Bank employees had completed between June 2009 and December 2011 for non-customer money transfers involving Western Union. The consultant concluded that, by failing to review IRFs between June 2009 and December 2011, the Bank had failed to file approximately 77 SARs.

- **Security Blanket.** The consultant also estimated that, if the Bank had held its monthly Security Blanket alert limit at 1,000 in the period between April 2006 and December 2008—rather than reducing the limit to 500—the Bank would have filed an additional 561 SARs. The consultant did not analyze how many additional SARs the Bank would have filed during that time period (beyond the 561 referenced above) if it had eliminated the monthly alert limit altogether. Neither did the consultant consider the effect of raising the alert limits for the capped Queries, even though the alerts from those Queries had historically produced a higher volume of SARs than the alerts from Security Blanket. The consultant did, however, consider a sample of 97 accounts with Security Blanket alerts that fell below US Bank's alert thresholds. It determined that 21 of those accounts (21.7%) were "productive or potentially productive," as that term is defined above.

- **The 90-Day Rule.** Finally, the consultant analyzed the impact of the Bank's 90-day rule, under which Queries on accounts that had generated an alert within the last 90 days would not generate a new alert, regardless of how suspicious the activity appeared to be or whether the prior alert resulted in a SAR. Considering three example Queries, the consultant estimated that, in 2013, the 90-day rule had caused US Bank not to investigate as many as 6,000 "productive" alerts.

68. The additional SARs that US Bank filed as a result of its look-back analysis addressed structuring, suspected financial crime, and other potential criminal activity.

C. US Bank Filed Thousands of Materially Inaccurate CTRs

69. Finally, from July 7, 2014 through May 27, 2015, US Bank filed 5,052 materially inaccurate CTRs that misidentified the ultimate beneficiaries of the relevant transactions.

70. Specifically, in the field where the Bank was supposed to identify by name the entity on whose behalf the transactions were being conducted, the Bank wrote the name of its customer (*i.e.*, a domestic respondent bank). However, the domestic respondent bank was not conducting the transactions on its own behalf, but rather on behalf of its customers' customers. In most cases, the respondent bank's customers were credit unions, and for at least $600 million of the currency transactions, the credit unions' customers (*i.e.*, the entities on whose behalf the transactions were being conducted) were MSBs.

71. The Bank knew that the ultimate beneficiaries of the transactions were MSBs because it included the MSBs' TINs in the CTRs. But it reported those TINs as belonging to the respondent bank. By filing the CTRs in this way, US Bank impeded law enforcement's ability to identify and track potentially unlawful behavior, as a search of the CTRs using the names of the relevant MSBs would have yielded no response. The transactions underlying these CTRs involved more than $600 million.

FIRST CLAIM FOR RELIEF

Violation of the Bank Secrecy Act
(31 U.S.C. § 5318(h) and 31 C.F.R. § 1020.210)
Anti-Money Laundering Program Violations

72. The Government incorporates by reference each of the preceding paragraphs as if fully set forth in this paragraph.

73. US Bank was required to implement and maintain an effective AML program, as set forth in the BSA and its implementing regulations.

74. As described above, from no later than 2011 to June 2014, US Bank failed to implement and maintain an effective AML program. Among other things, US Bank inappropriately capped the number of alerts it would investigate to uncover potentially

suspicious activity, failed to incorporate Western Union money transfers by non-customers into its automated monitoring system, employed a patently insufficient number of AML investigators, and failed to independently validate its AML monitoring systems.

75. US Bank's failures were willful within the meaning of the civil enforcement provisions of the BSA because Bank employees knew that its policies were inadequate and sought to hide that fact from the OCC, among others.

76. Under 31 U.S.C. § 5318(h), 31 U.S.C. § 5321(a), and 31 C.F.R. § 1020.210, US Bank's willful failure to implement and maintain an effective AML program renders it subject to a penalty of $25,000 per day.

77. As a result of the conduct set forth above, FinCEN is entitled under 31 U.S.C. § 5320 to an order requiring US Bank to meet with FinCEN annually for a period of two years to: (a) identify all remedial actions the Bank has taken during the preceding calendar year to address prior deficiencies related to its allocation of resources (including sufficient staff) to its BSA/AML Program, and explain why existing resource levels are sufficient to maintain compliance with the BSA; and (b) identify the independent testing that has been conducted (either internally or externally) during the preceding calendar year on the BSA functions at the Bank, including model validation of its transaction monitoring software and reviews of its processes and procedures regarding alert generation, investigation of alerts, and disposition of alerts.

SECOND CLAIM FOR RELIEF

Violations of the Bank Secrecy Act
(31 U.S.C. § 5318(g) and 31 C.F.R. § 1020.320(a))
SAR Reporting Violation

78. The Government incorporates by reference each of the preceding paragraphs as if fully set forth in this paragraph.

79. US Bank was required to file SARs on a timely basis, as set forth in the BSA and its implementing regulations.

80. As described above, the Bank failed to file timely SARs on thousands of suspicious transactions that a risk-based AML program would have identified and reported.

81. US Bank's failure to file timely SARs constituted a willful violation of the BSA and its implementing regulations because Bank officials knew, from below-threshold testing and other sources, that its deficient AML practices were causing it to fail to report suspicious activity.

82. Under 31 U.S.C. § 5318(g), 31 U.S.C. § 5321(a), and 31 C.F.R. § 1010.820(f), each transaction on which US Bank willfully failed to file a timely SAR renders it subject to a "civil penalty not to exceed the greater of the amount (not to exceed $100,000) involved in the transaction or $25,000."

83. As a result of the conduct set forth above, FinCEN is entitled under 31 U.S.C. § 5320 to an order requiring US Bank to meet with FinCEN annually for a period of two years to: (a) identify all remedial actions the Bank has taken during the preceding calendar year to address prior deficiencies related to its allocation of resources (including sufficient staff) to its BSA/AML Program, and explain why existing resource levels are sufficient to maintain compliance with the BSA; and (b) identify the independent testing that has been conducted

(either internally or externally) during the preceding calendar year on the BSA functions at the Bank, including model validation of its transaction monitoring software and reviews of its processes and procedures regarding alert generation, investigation of alerts, and disposition of alerts.

THIRD CLAIM FOR RELIEF

Violations of the Bank Secrecy Act
(31 U.S.C. § 5313(a) and 31 C.F.R. § 1010.311)
CTR Reporting Violation

84. The Government incorporates by reference each of the preceding paragraphs as if fully set forth in this paragraph.

85. US Bank was required to file complete and accurate CTRs on a timely basis, as set forth in the BSA and its implementing regulations.

86. As described above, US Bank filed 5,052 materially inaccurate CTRs that misidentified the entity on whose behalf the transaction had been conducted.

87. US Bank's failure to file accurate CTRs was willful because, in each instance, the Bank knew the entities on whose behalf the transactions were being conducted, but nevertheless failed to identify them properly in the CTRs.

88. Under 31 U.S.C. § 5313(a), 31 U.S.C. § 5321(a), and 31 C.F.R. § 1010.820(f), each transaction on which US Bank willfully filed a deficient CTR renders it subject to a "civil penalty not to exceed the greater of the amount (not to exceed $100,000) involved in the transaction or $25,000."

WHEREFORE, the Government respectfully requests that judgment be entered in its favor against Defendant, and that the Court:

(a) Issue an order reducing FinCEN's assessment against US Bank to judgment, and awarding the Government judgment in the amount of $185 million;

(b) Issue an order requiring US Bank to meet with FinCEN annually for a period of two years to: (a) identify all remedial actions the Bank has taken during the preceding calendar year to address prior deficiencies related to its allocation of resources (including sufficient staff) to its BSA/AML Program, and explain why existing resource levels are sufficient to maintain compliance with the BSA; and (b) identify the independent testing that has been conducted (either internally or externally) during the preceding calendar year on the BSA functions at the Bank, including model validation of its transaction monitoring software and reviews of its processes and procedures regarding alert generation, investigation of alerts, and disposition of alerts; and

(c) Award such further relief against Defendant as the Court may deem just and proper.

Dated: February 15, 2018
New York, New York

GEOFFREY S. BERMAN
United States Attorney for the
Southern District of New York
Attorney for Plaintiff

By: /s/Christopher B. Harwood

CHRISTOPHER B. HARWOOD
CALEB HAYES-DEATS
Assistant United States Attorneys
86 Chambers Street, Third Floor
New York, New York 10007
Telephone: (212) 637-2728/2699
Fax: (212) 637-2686
christopher.harwood@usdoj.gov
caleb.hayes-deats@usdoj.gov